The invention claimed is:

1. (Original) A method for producing a shortened representation of a collection of bits, comprising the steps of:

inputting the collection of "n" bits;

summing a key having at least "n" bits with the collection of bits to produce a sum;

squaring the sum to produce a squared sum;

performing a modular "p" operation on the squared sum, where "p" is at least as large as a first prime number greater than 2^n to produce a modular "p" result;

performing a modular 2^l operation on the modular "p" result to produce a modular 2^l result where, "l" is less than "n"; and

outputting the modular 2^l result.

2. (Original) A method for producing a shortened representation of a collection of bits, comprising the steps of:

inputting the collection of "n" bits;

summing a first key having at least "n" bits with the collection of bits to produce a first sum;

squaring the first sum to produce a squared sum;

summing the squared sum with a second key having at least "n" bits to produce a second sum;

performing a modular "p" operation on the second sum, where "p" is at least as large as a first prime number greater than 2^n to produce a modular "p" result;

performing a modular 2^l operation on the modular "p" result to produce a modular 2^l result where, "l" is less than "n"; and

outputting the modular 2^l result.

3. (Original) A method for producing a shortened representation of a collection of bits, comprising the steps of:

inputting a collection of "n" bits;

summing a key having at least "n" bits with the collection of bits to produce a sum;

squaring the sum to produce a squared sum;

repeating the previous three steps at least once to produce a plurality of squared sums, where a different key is used each time the steps are repeated;

summing the plurality of squared sums to produce a summation;

performing a modular "p" operation on the summation, where "p" is at least as large as a first prime number greater than 2^n to produce a modular "p" result;

performing a modular 2^l operation on the modular "p" result to produce a modular 2^l result where, "l" is less than "n"; and

outputting the modular 2^l result.